REMARKS

Claims 1-3, and 5-20 are active in the application. Claim 4 has been cancelled.

Claims 10 and 18 were objected to for not containing the word 'and' before the final element. This informality has been corrected.

Claims 3 and 12 were objected to for being indefinite for reciting the limitation "of large magnitude". Claims 3 and 12 have been amended to remove this limitation.

Other amendments have been made to claims 1, 10 and 18 to improve clarity and remove antecedent basis errors. No new matter has been added.

Claims 1-6, 8-14, and 16-20 were rejected under 35 USC 102(e) as being anticipated by US Patent 6,321,335 to Chu. This rejection is traversed by amendment. Claims 1 and 18 have been amended to recite that the electronic fuses are altered or programmed a second time. Claim 10 has been amended to recite that the electronic device is disabled by disabling an essential hardware component.

Claims 7 and 15 were rejected under 35 USC 103(a) as being unpatentable over Chu. This rejection is traversed by amendments to claims 1, 10 and 18.

The present invention provides a secure electronic device and method in which an electronic password or identification code is stored in an array or concatenated series of electronic fuses. The password can be burned into the device at the time of manufacture, or by the user, for example. An advantage of using fuses is that it is not possible to circumvent the fuse-based security feature by software techniques. Employing fuses for storing the password relies on hardware, and is therefore immune to software-based attacks.

One problem with employing fuses for storing passwords in an electronic device is that fuses are permanent. Once blown, fuses cannot be reset. However, in some instances it is desirable for a user to change a password. For example, if the password has been exposed, or if the device has been sold to a new owner, the new user may wish to change the password, but retain the security advantages inherent in a fuse-based password storage feature. Chu does not teach or suggest how to re-write or alter passwords encoded as blown fuses.

The present invention as claimed in amended claims 1 and 18 provides a method and device for simultaneously providing the benefits inherent in fused-based password storage (immunity to software based attacks), and alterability of the password. The ability to rewrite the fuse-encoded password is described in the present specification at page 12, lines 11-20. Independent claims 1 and 18 have been amended to requ alterability. Specifically, in the present invention, an update code is written over the original password. The combination of the update code and the original password create a new password. Specifically, the new password is the OR-function product of the original password and the update code. Using this method, the password stored on the device can typically be altered several times. Each time, additional fuses are blown as a new update code is added. And each time, the new password will be the OR-function product of the update code, original password, and all prior update codes.

By comparison, Chu teaches a personal computer that can permanently store a password or id code in a flash memory (which is alterable) or array of electronic fuses (which is not alterable). Chu does not teach or suggest altering the password or id code stored in the fuses. In fact, Chu teaches that the password stored in the fuse array is "permanent". For example, in Col. 9, lines 18-22, Chu mentions that the code can be "placed in the device by a <u>one time</u> programming techniques (sic) using, for example, fuses or the like." In col. 9, lines 23-25, and col. 11. lines 1-15, Chu teaches that the password is permanent. In col. 8, lines 48-59, Chu teaches that the password can be changed, but this aspect is specifically related to the use of flash memory, which is well known for its ability to be rewritten many times. Chu does not teach or suggest that the password can be changed or altered when it is stored in programmed fuses. Accordingly, the rejections of claims 1 and 18 are traversed by the present amendments and the rejections of these claims must be withdrawn.

Claim 10 has been amended to include the limitation that the electronic device is disabled by disabling an essential hardware component.

One problem with employing stored passwords is that the enable/disable function can sometimes be circumvented by software attacks. In other words, a software attack can enable the device even if the stored password does not match a password entered by a malicious user (i.e. a hacker). This is a possibility if the fuses are analyzed by a software application. In order to prevent this problem, the present invention may employ hardware-based enable/disable schemes. Hardware-based enable/disable schemes cannot be circumvented by software attacks. Specifically, in the present invention, the disable function (activated if an entered password does not match a stored password) operates by disabling one of three circuit elements essential to the device. Specifically, the present device can disable itself by: (1) disabling scan chains comprising the fuse elements, (2) disabling a phase lock loop required for operation (e.g. by disabling an enable port), or (3) disabling the system clock or clock distribution tree. Any of these disabling functions can be accomplished by applying appropriate signals to a gated buffer or an enable signal line on a critical component (see Fig. 7). The gated buffer or enable signal line can be controlled by the comparator that compares an entered password with the password stored in the fuses. With this hardware arrangement (which is inherently independent of software), the enable/disable function cannot possibly be affected by software based attacks; only hardware intervention can circumvent the disable feature. Hence, the present invention can be highly secure and immune to software-based attacks.

The present invention as claimed in claim 10 includes limitations requiring a hardware-based disable function. Specifically, claim 10 requires that, if an entered password (entered by a user attempting to gain access to the device) does not match a stored password (encoded in the concatenated fuses), then an essential hardware component is disabled. The essential hardware component can be a scan chain, a phase lock loop, or the system clock or system clock distribution. These specific aspects of the present invention are described at page 11, line 16 through page 12, line 10, and are illustrated in Fig. 7.

By comparison, Chu does not teach or suggest that the electronic device can be disabled by disabling essential hardware components. Chu does not teach that only hardware-based devices enable or disable the device. Instead, Chu teaches that software determines whether a match exists between stored and entered passwords, and that the software controls the disabling of the device. For example, col. 10, lines 1-6 teaches that a "security detection program" analyzes the password and controls the disabling of the device. Chu does not teach or suggest that the device can be disabled by any of the three specific methods required in claim 10: disabling gate scan chains, disabling phase lock loop, or disabling a system clock or clock distribution. Accordingly, the rejection of claim 10 is traversed by the present amendment and must be withdrawn.

With the present invention as now claimed in claim 10, the electronic device will be exceptionally secure because no possible software attack can undermine the password protection. The storage of the password (in electronic fuses), the detection of the password (by a comparator), and the disabling of the device (by gating the clock or other essential enable port) are all hardware based and cannot be manipulated by software-based techniques. Hence, the present electronic security technique is immune to software based hacking attacks. Chu does not teach the disabling features, which are expressed in claim 10 as amended.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1-3 and 5-20 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees for the petition or for entry of this amendment to Attorney's Deposit Account No. 09-0458 (International Business Machines Corporation).

Respectfully submitted,

Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis, & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA, 20190
Phone: 703-787-9400
Fax: 703-787-7557